UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/099,779	03/14/2002	Todd Weston Arnold	AUS920010984US1	4841

40412 7590 09/10/2007
IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN, TX 78709-0609

EXAMINER
WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/099,779	ARNOLD ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1, 6 – 8, 14, and 19 – 29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 6 – 8, 14, and 19 – 29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 12/07/2006.

All objections and rejections not set forth below have been withdrawn.

Claims 1, 6 – 8, 14, and 19 – 29 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 6 – 8, 14, and 19 – 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1, 8, and 14 each recite the limitation "the hardware security module identifier that is stored with the encrypted tied key". There is insufficient antecedent basis for this limitation in the claim. For the purpose of examination the examiner will presume the claims to recite "the stored hardware security module and the stored encrypted tied key".

All depending claims are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6 – 8, 14, and 19 – 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Al-Salqan, "Method and Apparatus for Encoding Keys", U.S. Patent, 6,549,626 in view of U.S. Department of Commerce (DOC), "Security Requirements for Cryptographic Modules" in view of Hosokawa, "Internet Broadcast Billing System", U.S. Patent Publication, 2001/0023416 A1 in view of Heer et al. (Heer), "Data Encryption Security Module", U.S. Patent 5,999,629.

Regarding claim 1, Al-Salqan discloses:

receiving, at a security module, a first password corresponding a software application (Al-Salqan, col. 2, lines 12-28, 49-63; fig. 2, elem. 204). Herein, Al-Salqan teaches that users may use computers to perform cryptographic applications. For example, to utilize a cryptographic key, a user may employ an application to provide a password, derive a key, and perform cryptographic operations upon data such as a file. The inventive method of Al-Salqan is for facilitating the operation of such application.

generating, at a security module, a first mask value based on the first password (Al-Salqan, col. 4, lines 29-46; fig. 2); *combining, at a security module, the first mask value with a first encryption key* (Al-Salqan, col. 4, lines 49-52; fig. 2);

encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key (Al-Salqan, fig. 2). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teachings ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05).

Al-Salqan discloses the returning of the encrypted tied key to what is termed the "user". While, the Applicants themselves also equate a software application to the "user" (Instant Application, pg. 2, line 19 – pg. 3, line 2), the examiner notes that Al-Salqan does not explicitly state that a software application is represented by "the user" - hence, *returning the encrypted tied key to the software application.*

DOC more clearly shows that a user employs a software application to interact with a security module inside a computer. DOC teaches that a security module provides cryptographic services to software applications employed by users (iv, #8; pg. 27, sect. 4.6). When a user requests cryptographic services from a security module, the software application representing the user communicates with the security module using an application program interface (pg. 14, sect. 4.2; pg. 27, 28, iv).

It would have obvious to recognize the teachings of DOC, that a human employs a software application to interact with a security module within a computer, along with the teachings of Al-Salqan. This would have been obvious because one of ordinary skill in the art would have been motivated to practically provide a means for a human to accomplish a cryptographic application in cooperation with a security module inside a computer.

The combination enables:

sending the encrypted tied key and a second password from the software application to the security module over a computer network, the second password being the same as the first password (Al-Salqan, fig. 3, elems. 302,306). Herein, the combination discloses that the software application transmits the correct password and a corresponding tied key to the security module.

receiving, at the security module, the encrypted tied key and the second password from the software application; in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second key, the combining resulting in a recovered tied key (Al-Salqan, fig. 3). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teachings ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05).

generating a second mask value based on the second password (Al-Salqan, col. 4, lines 29-46; fig. 3). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teachings ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05);

separating a recovered encryption key from the recovered tied key using the second mask value (Al-Salqan, col. 7, lines 45-49; fig. 3). Furthermore, the applicant is kindly reminded of the evidence submitted by the applicant's representative, admitting to the Prior Art's (Al-Salqan) teaching of the recovery of an recovered encryption key from the recovered tied key ("Prior Art Flow Diagram", Telephonic Interview, 11/15/05).

and encrypting data provided by the software application using the recovered generated key (Al-Salqan, Abstract, lines 1-3; col. 1, lines 21-28; col. 2:15-22; col. 3, lines 52-56; DOC, pg. iv, #8). Herein enabled by the combination, is an application that takes data and a recovered key, and facilitates the performance of cryptographic operations such as encryption and decryption.

The combination discloses a system designed to ensure the secrecy of a data encryption key, such as a symmetric key. Secrecy is accomplished by encrypting the data encryption key. However, though the combination discloses enabling the secrecy of a symmetric data encryption key, it does not disclose the enabling of the authenticity of the key. Thus, the combination does not disclose wherein the first "encryption key" *is derived from a generated key and a known value the combining resulting a tied key* or that the recovered "encryption key" includes *a recovered generated key and a recovered known value.*

Hosokawa discloses a method for the verification of the authenticity of a data-encryption key, the method being performed "as a security measure" (Hosokawa, par 37). This "security measure" of ensuring authenticity is additional to the security measure of ensuring secrecy - encrypting the data encryption key. The method comprises the creation of a "tied key", or an "encryption key" derived from a generated key and a known value (Hosokawa, par. 32, lines 8-12; par. 33, lines 1-5; par. 37, lines 11-13; par. 44, lines 11-18). Hosokawa attaches a "known value", a digital signature, to generated key, and thereby creates a "tied key". After the "tied key" is decrypted, the attached digital signature is compared to an authentic digital signature so as to verify the authenticity of the generated key. If authentic, the generated key is used for encrypting data. Thus, Hosokawa discloses a method usable to verify the authenticity of an encryption key, the method ensuring a measure of security.

It would have been obvious to one of ordinary skill in the art to combine the method of Hosokawa with the system of the combination of Al-Salqan and DOC. This would have been obvious because one of ordinary skill in the art would have been motivated to enhance the security of the system of combination, by not only enabling the secrecy of the data encryption key, but also the authentication of the data encryption key. Thus, a more secure system is provided.

The combination does not appear to explicitly recite the added limitations of *storing, by the software application, the encrypted tied key and a hardware security module identifier that identifies the security module; determining, by the software application, that the encrypted tied key corresponds to the security module based upon the hardware security module identifier that is stored with the encrypted tied key.*

However, Heer discloses that it was already well established for software applications that employ security modules for security to store encrypted keys along with a corresponding hardware security module identifier (fig. 1:20; 3:45-61). When the need arises to utilize the key, the software application will determine the association of the encrypted key and the hardware security module identifier.

It would have been obvious to one of ordinary skill in the art to employ the established teachings of Heer within the combination of Al-Salqan, DOC, and Hosokawa. This would have been obvious because one of ordinary skill in the art would have been motivated by the flexibility and added security provided by a system that can provide a plurality of system users with the safe utilization of encrypted keys via the cooperation of hardware security modules and facilitating software applications.

Regarding claim 6, the combination disclose:

determining whether the recovered known value is correct; and processing a data file based on the determination (Hosokawa, col. 2, pars. 32, 33; Al-Salqan, Abstract, lines 1-3; col. 7, lines 37-49; col. 3, lines 52-56).

Regarding claim 7, the combination disclose:

wherein the processing is selected from the group consisting of encrypting the data file using the recovered generated key and decrypting the data file using the recovered generated key (Al-Salqan, Abstract, lines 1-3; col. 7, lines 37-49; col. 3, lines 52-56).

Regarding claim 22, the combination disclose:

wherein the generated key is at a level of security corresponding to a sensitivity level of the data being encrypted (Hosokawa, par. 41). The combination disclose that the key is appropriately used for securing data, thus the key is at a level of security suitable for securing sensitive data.

Regarding claims 25 and 28, they are the system means and computer program product claims implementing the method of claim 22, and they are rejected, at least, for the same reasons.

Regarding claims 8, 14, 19, and 20, they are the system means and computer program product claims implementing the method of claims 1, 6, and 7, and they are rejected, at least, for the same reasons. Further, regarding claim 8 specifically, it is rejected because the combination disclose:

one or more processors; a memory accessible by the processors; one or more nonvolatile storage devices accessible by the processors; a hardware security module accessible by the processors; a data security tool for securing data using the hardware security module (Al-Salqan, figs. 1, 2; col. 3, lines 16-45).

Regarding claims 21 and 23, the combination disclose:

wherein the security module is a separate hardware security module and *wherein encrypting the data is performed within the security module* (DOC, pg. 5, lines 4-6; pg. 16, sect. 4.3.2).

Regarding claims 24, 26, 27, and 29, they are the system means and computer program product claims implementing the method of claims 21 and 23, and they are rejected, at least, for the same reasons.

Response to Arguments

Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

See Notice of References Cited.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J. Williams
AU: 2137
JW

CYNTHIA BRITT
PRIMARY EXAMINER
9-4-07